UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

BRENDA CZECH, individually and on behalf of a class of similarly situated individuals, Plaintiff, v. WALL STREET ON DEMAND, INC., a Delaware corporation, and JOHN DOES, Defendants.	No. 09-CV-00180 (DWF/RLE) DEMAND FOR JURY TRIAL CLASS ACTION

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Brenda Czech, by and through her undersigned attorneys, brings this class-action complaint against Defendants to stop their practice of transmitting unauthorized text messages to the wireless devices of consumers nationwide, and to obtain redress for damages suffered by her and all persons injured by defendants' conduct. For her class-action complaint, Plaintiff alleges as follows on personal knowledge regarding herself and her own acts and experiences, and, regarding all other matters, on information and belief, including the investigation conducted by her attorneys.

PRELIMINARY STATEMENT

1. Defendant Wall Street On Demand, Inc. ("WSOD") is a financial information service company that provides, among other things, services to its clientele of securities brokerage houses and other financial concerns primarily over the Internet

and through software applications. WSOD is in the business of, among other things, developing, designing, and hosting custom websites, reports, and other tools for the financial industry.

2. One such software application owned and operated by WSOD is the financial-information service referred to herein as Watch List Alert, which transmits electronic text messages (e.g., SMS or "Short Message Services") to the wireless devices of end-user consumers worldwide.

3. WSOD operates in the extremely competitive market of financial information service providers, all of whom, including WSOD and its affiliates, compete for clients such as The Vanguard Group, Inc. and Investor's Business Daily, Inc., among others.

4. To provide additional functionality for its users, and possibly to obtain additional revenue, WSOD allows users of Watch List Alert to input wireless telephone numbers into their Watch List Alert accounts so that communications received by the account will be forwarded as text messages ("SMS" or "text messages") to the wireless telephone numbers inputted into the account.

5. Watch List Alert's text-message-service feature contains a major flaw, which WSOD has known about for some time: Watch List Alert automatically sends text messages to whatever wireless phone number(s) a particular user enters into his Watch List Alert account, regardless of whether the person receiving the text messages actually wants to receive or has authorized receiving the text messages. For example, new wireless-device customers commonly receive previously used or "recycled" wireless-

telephone numbers, some of which customers then receive from WSOD unauthorized and unwanted Watch List Alert text messages.

6. WSOD's rush to outmaneuver its competitors and to make a profit has inconvenienced and damaged wholly innocent, uninvolved third parties – including Plaintiff – who have received and continue to receive unwanted, unauthorized text messages from WSOD. Those innocent persons who receive these unauthorized text messages also have to pay for the text messages, even though they are completely unauthorized and unwelcome.

7. To redress these injuries, Plaintiff Brenda Czech, on behalf of herself and a nationwide class of wireless-device users, brings this Complaint under the Computer Fraud & Abuse Act, 18 U.S.C. § 1030, et seq., as amended by Identity Theft Enforcement & Restitution Act of 2008, P.L. No. 110-326 ("CFAA"), and the common law of the several States, and seeks damages and injunctive relief enjoining Defendants' future unlawful conduct as described herein.

PARTIES

8. Plaintiff Brenda Czech is an individual residing in and a citizen of Stearns County, State of Minnesota.

9. Defendant Wall Street On Demand, Inc. ("WSOD") is a financial information services company. WSOD is a corporation organized and existing under the laws of the State of Delaware with its principal place of business in the State of Colorado. WSOD conducts its business throughout the United States, including the State of Minnesota.

10. Defendants John Does ("Does"), who are presently unknown to Plaintiff, are one or more individuals or corporations transmitting the unauthorized text messages at issue in this case. Plaintiff is informed and believes, and on that basis alleges, that each of these fictitiously-named Defendants are in some manner responsible for the acts, omissions, injuries, and/or damages alleged in this Complaint. Plaintiff will seek leave to amend this Complaint to allege the true names and capacities of these fictitiously-named Defendants when the same have been ascertained.

JURISDICTION & VENUE

11. This Court has subject-matter jurisdiction over this action because Plaintiff asserts claims under the federal Computer Fraud & Abuse Act, 18 U.S.C. § 1030, et seq., as amended by Identity Theft Enforcement & Restitution Act of 2008, P.L. No. 110-326 (hereinafter "CFAA").

12. This Court also has subject-matter jurisdiction over this action under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §§ 1332, 1441, 1446, and 1453 (2005), because, among other things (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; (2) there are at least 100 members of the putative nationwide class Plaintiff seeks to represent; and (3) at least one member of the putative class is a citizen of a state different from that of Defendants. Upon information and belief, Defendants have collected more than $5 million directly or indirectly from their unauthorized text messages sent to Plaintiff and members of the Class.

13. This Court also has supplemental jurisdiction over Plaintiff's state-law claims under 28 U.S.C. § 1367, because these claims arise out of the same common nucleus of operative fact as Plaintiff's federal claims, and would ordinarily be expected to be tried in one judicial proceeding.

14. This Court has personal jurisdiction over Defendants because all or part of the transactions giving rise to this lawsuit occurred in this District.

15. Venue is proper under 28 U.S.C. § 1391 because Plaintiff resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims have occurred and/or a substantial part of the property that is the subject of this action is situated in this District.

FACTUAL BACKGROUND

WSOD's Watch List Alert

16. In or around 2006, WSOD first released the current software version of its Watch List Alert, and has routinely updated the software since that time.

17. Watch List Alert's mobile or text-messaging feature employs technology known as Short Message Services ("SMS"), which is an information-delivery system that allows users of wireless devices, such as cellular telephones and personal-digital assistants (e.g., Palm Pilots and Blackberrys), to send and receive short text messages, which usually are limited to around 160 text characters.

18. The first SMS text messages were sent during 1992 and 1993, although text messaging was not widely offered or used on a commercial basis until around 2000. According to a March 23, 2009 Congressional Research Service report, however,

approximately 48 billion text messages are sent each month in the United States. (http://assets.opencrs.com/rpts/RL34632_20090323.pdf)

19. Watch List Alert's text-messaging feature works primarily by transmitting stock updates and related financial information. WSOD converts that financial information into text messages, which it then sends with the assistance of unknown third-parties (i.e., Defendants Does) to cellular telephones or wireless devices. In doing so, WSOD controls the length and format of the text messages by, among other things, changing both the format and content of the financial information before transmitting it as text messages.

20. Watch List Alert has a significant user base: thousands of Watch List Alert users legitimately take advantage of its text-messaging features.

21. To obtain the necessary technical expertise and/or billing relationships to operate Watch List Alert's text-messaging feature, WSOD (itself or through its agents such as m-Qube, Inc., mBlox Inc., Verisign Inc., and/or others ("aggregators")), partners with national cellular telephone carriers such as AT&T Mobility, Sprint, T-Mobile, and Verizon ("wireless carriers").

22. Under their contracts with a wireless carrier, recipients of Watch List Alert text messages generally must pay either a per-message fee or a flat rate to receive the text messages. Recipients of Watch List Alert text messages, however, like Plaintiff and the members of the Class, are charged text-message fees (or their monthly text-message plans are depleted by the number of text messages received from WSOD) even if the

wireless-device users did not give WSOD their prior consent to receive the Watch List Alert text messages.

23. WSOD and/or the wireless carriers profit from Watch List Alert's text-messaging feature by charging recipients of the text messages a fee to receive the text messages. Fees vary in amount; however, they are typically around $0.15 per text message. WSOD also profits from contracts with its content-provider clients and affiliates, among others, which pay WSOD a per-text-message fee or a contractually negotiated flat-rate text-message fee for sending Watch List Alert text messages to recipients whether or not the recipients, like Plaintiff and the members of the Class, actually consented to receive the text messages from WSOD.

24. Consequently, WSOD has a financial incentive to send as many Watch List Alert text messages as possible to users of wireless devices, regardless of whether the users actually consented to receive the text messages from WSOD.

25. Defendants and/or their aggregator partners also levy additional fees for various forms of text-message content, which fees appear on consumers' cellular-telephone bills as separate line-item charges. Many of these charges are similarly unauthorized.

26. In addition to the above-described text-message fees, during the relevant period Watch List Alert's unauthorized text-message content, among other things: (1) caused the wireless devices of Plaintiff and the members of the Class to slow and/or lag in operation; (2) consumed/took up the wireless bandwidth of the wireless devices of Plaintiff and the members of the Class; (3) depleted the memory of the wireless devices

of Plaintiff and the members of the Class; and (4) frustrated Plaintiff and the members of the Class. All of these are the result of the receipt of unauthorized text-message content, among other things, and impaired the availability of and interrupted the wireless-device service of Plaintiff and the members of the Class regardless of their particular wireless-carrier provider.

27. For example, handheld wireless devices, in contrast to modern personal computers, have relatively limited random-access or random-operating memory ("RAM" or "ROM"). When a wireless device receives an unauthorized text message, the wireless device's finite RAM or ROM is depleted or "used up," causing the device's other electronic operations and functioning (including the user's receipt of legitimate text-message content) to slow or lag in operation, or actually lock up completely, which impairs the integrity and availability of data, program(s), system(s), or information found in or on a consumer's wireless device, including the wireless devices of Plaintiff and the members of the Class.

28. Under certain circumstances, unauthorized text messaging, such as the text messaging by WSOD, also can cause a wireless device to shut down completely and automatically reset, with the result being the device rebooting itself, reformatting the memory of wireless device, and erasing any stored information on the device's permanent storage or "hard drive."

29. The impairment to the RAM or ROM of wireless devices resulting from unauthorized text messaging such as the text messages sent by WSOD to Plaintiff and the members of the Class is not theoretical. According to the Attorney General of Michigan,

for example, receiving unauthorized text messages is not only annoying to the user but "it can also slow down [the user's] phone by taking up [the user's] phone's memory and, unlike spam e-mail, lead to unwanted charges on [the user's] wireless service bill." (http://www.michigan.gov/ag/0,1607,7-164-34739_20942-190608--,00.html)

30. Handheld wireless devices, in contrast to modern personal computers, also operate on limited wireless bandwidth (as opposed to Internet bandwidth, which is commonly ubiquitous depending on the user's particular Internet Service Provider). When a wireless device is in the process of receiving an unauthorized text message, wireless bandwidth that would otherwise be dedicated to other wireless operations such as the user's telephone calls, internet access, instant messaging, or the user himself sending or receiving a legitimate text message, is misallocated, interfered with, and/or depleted, which impairs the integrity and availability of data, program(s), system(s), or information found in or on a consumer's wireless device, including the wireless devices of Plaintiff and the members of the Class.

31. In addition, handheld wireless devices, unlike modern personal computers, also have relatively finite permanent or "hard drive" memory storage capacity. Consequently, the more unauthorized text messages a wireless device receives the more finite hard drive storage capacity of a wireless device is temporarily and/or permanently misallocated, depleted, or consumed, which causes, among other things, the wireless device to slow or lag in its operation or functioning, or otherwise shutdown completely, which impairs the integrity and availability of data, program(s), system(s), or information

found in or on a consumer's wireless device, including the wireless devices of Plaintiff and the members of the Class.

32. Unauthorized text messages also have the capability of providing an "opening" to criminals or other malicious persons to break into a user's wireless device to use the device for nefarious purposes or to otherwise obtain information from the device. According to an industry presentation on July 30, 2009 at the Black Hat Security Conference in Las Vegas, Nevada, unauthorized text messaging can result in wireless-device users having "the[ir] smartphones knocked offline, commanded to visit sites hosting pornography or viruses, or even turned into remote-controlled subordinates of a criminal gang behind an attack."

33. One co-presenter at the conference, for example, demonstrated how he could disconnect an iPhone from a cellular network by sending it a single, maliciously crafted text-message – a message that the victim never even sees when it is received by the wireless device. The text messages can exploit bugs in the way the iPhone handles certain messages and can be used to crash parts of the iPhone's software. The conference presenters also demonstrated that it is possible to remotely control an iPhone by sending 500 messages to a single victim's phone.

34. According to the conference presenter, unauthorized text messaging potentially is a "powerful attack vector." He continued: "All I need to know is your phone number. As long as [the user's] phone's on, I can send this [the text message] and their phone's going to do something with this [the text message] . . . . It's always on, it's

always there, [and] the user doesn't even have to do anything – it's the perfect attack vector."

35. Unauthorized text messages also pose particular problems for wireless-device users, such as Plaintiff and the members of the Class, that far exceed the problems for users resulting from unwanted or "spam" e-mail sent indiscriminately to users of personal computers. Beyond being levied a per-message charge or flat-rate fee per text message received, which a recipient of unwanted or "spam" e-mail usually does not incur, wireless-device users, like Plaintiff and the members of the Class, generally are not able to (in Plaintiff's case, she could not) take advantage of spam filters, "junk e-mail" programs, and other security devices designed specifically to block or quarantine unwanted or "spam" e-mails sent to personal computers.

36. In other words, in contrast to unwanted or "spam" e-mail, there is no way for a wireless-device user, such as Plaintiff or a member of the Class, to block or filter unwanted or unauthorized text messages from being sent to his wireless device(s), other than to possibly contact the user's wireless carrier and instruct or request that the carrier (at a possible cost to the user) deactivate the wireless-device's text-messaging functionality altogether.

37. By forcing wireless-device users, including Plaintiff and the members of the Class, to expend time and effort attempting to delete or otherwise remove Watch List Alert text messages from their wireless devices and to stop future text messaging from WSOD, Watch List Alert decreased the productivity of Plaintiff and the members of the Class. The cumulative impact of not only the multiple unwanted text messages from

WSOD, but also the threat that they would continue to be received along with the accompanying text-messaging charges, substantially impaired the use of the wireless devices of Plaintiff and the members of the Class.

38. In addition to the above-described problems resulting from unauthorized text messaging, government regulation in this area is in its infancy, making actions such as this one essential to protect users of wireless devices, such as Plaintiff and the members of the Class.

39. For example, unauthorized commercial SMS text messaging is only partly restricted by the federal government's "Do Not Call" and CAN-SPAM regulations (http://www.fcc.gov/cgb/consumerfacts/canspam.html). The federal government's CAN-SPAM regulations generally prohibit unauthorized text messaging using the SMTP protocol (text-message protocol where text messages are identified by an Internet address that includes an Internet domain name).

40. Many unauthorized SMS text messages, however, are sent using the SMPP text-message protocol, which the CAN-SPAM Act does not regulate. *Id*. ("The FCC's ban does not cover short messages . . . that do not use an Internet address.")); (http://assets.opencrs.com/rpts/RL34632_20090323.pdf). Thus, text messages sent using the SMPP text-message protocol currently are free of regulation under the federal government's CAN-SPAM and "Do Not Call" regulations.

41. Acknowledging this loophole, on April 2, 2009, Senators Olympia Snowe and Bill Nelson introduced the m-SPAM Act 2009 (Sen. R. No. 788). The m-SPAM Act would strengthen the FCC's and FTC's power to curb unwanted text messages using any

text-message protocol (including the SMPP protocol) and would protect consumers by strictly prohibiting persons from sending commercial text messages to wireless numbers listed on the national Do-Not-Call registry.

42. In announcing the legislation, Senator Nelson observed: "Spam e-mail is bad enough . . . . Now we are seeing a proliferation of unwanted messages – and consumers are getting stuck paying." The Senators' press release announcing the legislation also described the damage to wireless devices and cost to consumers resulting from unwanted text messaging: "M-spam not only clutters a wireless user's inbox, but it also unduly increases the [user's] monthly bill – wireless subscribers typically are charged for sending and receiving text messages – sometimes as much as 20 cents per message."

43. Beyond causing various forms of damage to wireless devices, unauthorized text messages, such as those sent by WSOD, also allow the sender of the text message to obtain information from the wireless-device user, including Plaintiff and the members of the Class.

44. Wireless-carriers generally do not publish or otherwise publicly disseminate wireless-telephone numbers, including to those persons seeking to exploit commercially those wireless numbers for marketing and/or advertising purposes. In addition, a wireless-device user generally can block marketers from actually calling a wireless number by subscribing to the national "Do No Call" registry.

45. But if a text message is successfully sent to a wireless device, as opposed to being "bounced back" from the user-recipient (similar to an undeliverable e-mail), the

person sending the text message obtains information (through a read- or delivery-receipt or other delivery notification) that the wireless number is active, the general geographic area where the user is located (via the information obtained through simple analysis of the wireless number's area code), and that future text messages can be sent to that active wireless number. In some cases, ever evolving wireless-user-location technology (such as Google Latitude (http://www.google.com/mobile/products/latitude.html#p=default)) can potentially allow the sender of a text message to obtain information regarding the *actual* physical location of the wireless-device user.

46. Knowing that a particular wireless number is active and the general or actual geographic location of the wireless-device user, including Plaintiff and the members of the Class, also allows the sender of a text message, such as WSOD, to sell, license, or otherwise market that wireless number to others, including clients or affiliates of the sender, such as those clients or affiliates contracting with WSOD, who wish to send related text-message content to that active wireless number. For example, the Mobile Information Access Company is one company that compiles databases of wireless numbers for certain clients and then sells, licenses, or markets those numbers to other persons for commercial marketing purposes.

47. The information obtained by senders of text messages such as WSOD who determine that a wireless-number is active also allows commercial senders of text messages, such as WSOD, to evade the restrictions on making unsolicited commercial-marketing telephone calls to wireless numbers registered on the government's "Do Not

Call" list and lets senders such as WSOD circumvent the restrictions on sending unauthorized text messages under the CAN-SPAM Act.

48. For wireless-devices users who do not have a text-messaging plan, or have wireless devices that do not support text messaging, it also is possible for these users still be charged for "receiving" text messages even though they are not actually aware that they received the text messages.

49. WSOD knowingly provides no effective safeguard to ensure (or even attempt to ensure) that recipients of Watch List Alert text messages are not receiving and paying for unauthorized text messages. In fact, Watch List Alert's text-messaging feature is vulnerable to simple problems.

50. For example, when a WSOD wireless-device user terminates his wireless service with a national carrier, the wireless carrier is required by federal law to either "port" the user's wireless number to the user's new wireless carrier or "recycle" the user's wireless number for future use by a new wireless-device user. *See* 47 C.F.R. § 52.15(f)(ii).

51. Every month approximately 1.5% of wireless-device users terminate their service with their wireless carrier, leaving their wireless number to be "recycled" and given to another or new wireless subscriber. Prior to reassigning the number, however, the wireless carriers fail to "clean" the number, or remove it from any text-messaging services, such as WSOD's Watch List Alert, for which the number had been previously registered by the owner of the number.

52. Upon information and belief, Watch List Alert users terminate their wireless-carrier service at rates consistent with the national average above but fail to update or delete their old or discontinued wireless numbers from their Watch List Alert account.

53. Because WSOD knowingly neither tracks recycled wireless numbers nor provides, offers, or supports any way to verify a wireless-carrier user's continuing consent to receive text messages, Watch List Alert knowingly continues to transmit automatically text messages to new users of "recycled" wireless numbers – persons who have never consented to receive such messages.

54. Every month Watch List Alert knowingly transmits text messages to hundreds or thousands of wireless users who have not agreed to receive Watch List Alert text messages.

55. The problem of "recycled" wireless telephone numbers is not specific to WSOD. Other providers of text-messaging services similar to WSOD's have recognized the problem of recycled wireless telephone numbers and have taken steps to eliminate or minimize the problems caused by those numbers.

56. For example, in 2006, the popular social-networking website Facebook implemented a recycled wireless-number program with AT&T and Verizon where the two national wireless carriers agreed to provide Facebook Mobile with periodic notices of wireless numbers that had been deactivated by their users.

57. Despite initial technical hiccups, both AT&T and Verizon have provided deactivation notices to Facebook Mobile since at least 2006, which notices, upon

information and belief, AT&T and Verizon continue to generate and send to Facebook Mobile to the present day. Using the deactivation notices, Facebook Mobile is able to continually clean its database of recycled wireless numbers, and thereby eliminate or minimize its sending of unauthorized text messages to new users of recycled wireless telephone numbers.

58. In 2007, Facebook also reached a settlement in an action alleging that it sent unwanted and unauthorized text messages to thousands of wireless-device users who were assigned recycled numbers of Facebook users. A published report of the settlement in that case noted that the case "highlighted the problems that can arise as Websites extend their services to mobile handsets with phone numbers that have been reassigned after another customer's service ended."

59. Recognizing the industry-wide problem of wireless-device users being charged for text messages they did not authorized, the company mBlox recently introduced a new "Free to End User" text-messaging service that allows companies, such as WSOD, to send text-messages to wireless users without the end user having to pay a fee to receive the text messages. Using this "Free to End User" service, a company sending a text message absorbs the cost to the end user for the text messages. Currently, mBlox is working with T-Mobile and AT&T to provide this "Free to End User" service, and it plans to roll out the service to other wireless carriers in the future.

60. Despite its knowledge of the commercial availability and viability of such deactivated/recycled wireless-telephone-number programs such as the program used by Facebook Mobile, and the new "Free to End User" text-messaging services such as the

one marketed by mBlox, WSOD has knowingly failed and continues to knowingly fail to implement any such programs or services to prevent it from knowingly sending unauthorized text messages to users of recycled wireless numbers, such as Plaintiff and the members of the Class.

Allegations Specific To Plaintiff

61. In or about 2006, Plaintiff purchased new cellular-telephone service for her personal use from Sprint.

62. At that time, as part of her cellular-telephone-service plan, Sprint assigned Plaintiff a wireless telephone number and Plaintiff agreed to pay a monthly fee for a period of approximately 12 months.

63. During the relevant period, Plaintiff paid Sprint $39.95 per month for a 1000 anytime minutes plan plus an additional $5.00 per month for a "bucket" plan of 300 text messages per month. Under her bucket plan, if Plaintiff exceeded the 300 text messages (either sent or received) in any given month, she would be charged an additional $0.10 per text message. As part of her plan, therefore, Plaintiff paid Sprint a quantifiable amount for each text message she sent or received (i.e., $5.00/300, or $0.017 per message if she sent or received the total 300 messages) from her wireless device.

64. Shortly after activating her cellular-telephone service, Plaintiff's cellular-telephone account began receiving numerous Watch List Alert text messages, messages that Plaintiff neither wanted nor authorized. Plaintiff ultimately determined that the text messages originated from WSOD and, specifically, WSOD's Watch List Alert text-messaging service.

65. For example, in or about February 2008, Plaintiff received on her cellular telephone a Watch List Alert text message promoting a Watch List Earnings update for one of WSOD's numerous retail brokerage house customers.

66. Plaintiff's cellular-telephone account identified the source of the text messages as the domain name alerts.wallst.com, property at all relevant times licensed to and operated by WSOD.

67. Upon information and belief, because plaintiff did not authorize WSOD to send her this text message, and because the text message was sent using a SMTP protocol (text-message protocol where the message is identified by an Internet address that includes an Internet domain name), WSOD sent this unauthorized text message in violation of the Federal CAN-SPAM Act.

68. At no time did Plaintiff authorize or otherwise consent to receive WSOD's text messages on her cellular telephone.

69. The unauthorized text messages Plaintiff received from WSOD substantially interrupted the functioning of Plaintiff's cellular telephone and impaired the integrity and availability of data, program(s), system(s), or information found in or on Plaintiff's cellular telephone.

70. For example, the unauthorized text messages Plaintiff received from WSOD depleted or "used up" the phone's finite RAM or ROM and caused the phone's electronic operations and functioning to slow and lag in operation and functioning.

71. The unauthorized text messages Plaintiff received from WSOD also resulted in the misallocation, interference, or depletion of Plaintiff's cellular telephone's

limited wireless bandwidth that would otherwise have been dedicated to Plaintiff's other wireless operations such as Plaintiff's incoming and outgoing telephone calls, internet access, instant messaging, and Plaintiff's own sending or receiving of legitimate text messages.

72. The unauthorized text messages Plaintiff received from WSOD also resulted in the temporary and/or permanent misallocation, depletion, or consumption of Plaintiff's cellular telephone's finite permanent or "hard drive" memory storage capacity, which also caused Plaintiff's cellular telephone to slow or lag in its operation and functioning.

73. WSOD also knowingly obtained information from Plaintiff's cellular telephone as the result of sending unauthorized text messages to Plaintiff's phone. By sending unauthorized text messages to Plaintiff's cellular telephone, WSOD obtained information that Plaintiff's cellular telephone was active and functioning, and obtained information regarding the general and/or actual geographic location of Plaintiff's cellular telephone. Upon information and belief, WSOD used or could have used that information obtained from Plaintiff's cellular telephone to sell, license, or otherwise market Plaintiff's wireless-telephone number to WSOD's clients or affiliates interested in sending related text-message content to Plaintiff's cellular telephone.

74. WSOD also knowingly obtained information from Plaintiff's cellular telephone in the form of obtaining a portion of the finite permanent or hard drive memory storage capacity of the phone.

75. In addition to impairing the integrity and availability of data, program(s), system(s), or information found in or on Plaintiff's cellular telephone, and the information obtained by WSOD from Plaintiff's cellular telephone, WSOD's unauthorized text messages also depleted Plaintiff's per-month "bucket" text-message plan with her wireless carrier.

76. Under Plaintiff's contract with Sprint, she was allocated a finite number of text messages to send from or receive on her wireless device during any particular month, which text messages appeared as line-items on Plaintiff's bill from Sprint. Because of the unauthorized text messages from WSOD, the number of text messages Plaintiff was entitled to send or receive during a particular month was reduced by the number of unauthorized text messages she received from WSOD.

77. Despite repeated attempts over several weeks to stop the Watch List Alert text messages, Plaintiff was unable on her own to stop the text messages from Defendants. Eventually, with the assistance of legal counsel, a WSOD representative and/or Watch List Alert Technical Support person was finally able to "take steps" to ensure that Plaintiff would no longer receive Watch List Alert text messages.

78. WSOD ultimately suspended any future text messages to Plaintiff's wireless-device.

79. All of these actions taken by Plaintiff were taken by Plaintiff to remedy, among other things, the interruption of service to Plaintiff's cellular telephone resulting from WSOD's numerous unauthorized text messages.

CLASS ALLEGATIONS

80. Plaintiff Czech brings this action pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3), on behalf of herself and a class (the "Class") consisting of:

> All wireless-device subscribers in the United States who suffered losses or damages as a result of receiving unauthorized SMS or text messages on their wireless devices from, or on behalf of, Defendants provided, however, that the following are excluded from the proposed Class: (i) Defendants; (ii) any employee(s) of Defendants; and (iii) the District Court Judge assigned to this action.

81. The members of the Class are so numerous and geographically dispersed across the United States that joinder of all members of the Class would be impracticable. Members of the Class are located throughout the United States. The exact number of Class members is unknown to Plaintiff at this time, but Plaintiff reasonably believes the Class numbers at least in the thousands.

82. Plaintiff's claims are typical of the members of the Class. Plaintiff and all members of the Class were commonly impacted and damaged by Defendants' wrongful conduct.

83. Plaintiff will fairly and adequately protect the interests of the Class. The interests of Plaintiff are coincident with, and not antagonistic to, those of the Class. In addition, Plaintiff's counsel is experienced and competent in prosecuting complex class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class, and have the financial resources to do

so. Neither Plaintiff nor her counsel has any interest adverse to the other members of the Class.

84. Defendants have acted on grounds generally applicable to Plaintiff and the entire Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

85. Absent a class action, members of the Class would find the cost of litigating their claims to be prohibitive, and will have no effective remedy. Class treatment of common questions of law and fact also is superior to multiple individual actions or piecemeal litigation, in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

86. The Class has a high degree of cohesion, and prosecution of the action through class representatives would be unobjectionable. Plaintiff is not aware of any other difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

87. The factual and legal bases of Defendants' liability to Plaintiff and to the Class are the same, resulting in injury to Plaintiff and to the Class. Plaintiff and the other members of the Class all have suffered harm and damages as a result of Defendants' unlawful and wrongful conduct.

88. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class. Questions of law and fact common to the Class include, but are not limited to the following:

(a) Whether Defendants' conduct described herein is governed by the CFAA;

(b) Whether Defendants' conduct violates the CFAA;

(c) Whether Defendants have unjustly received money belonging to Plaintiff and the Class and whether principles of equity and good conscience dictate whether Defendants should be permitted to retain it;

(d) Whether Defendants' conduct amounts to trespass to chattels;

(e) Whether Defendants are required to institute policies and procedures to ensure that their text-message services have been authorized by the user; and

(f) Whether Defendants are required to institute policies and procedures to ensure that their text-message services can be cancelled upon request and refunds are available for any unauthorized text-message charges.

COUNT I
VIOLATION OF THE COMPUTER FRAUD & ABUSE ACT
(AGAINST ALL DEFENDANTS)

89. Plaintiff restates and realleges paragraphs 1-88 above as though set forth in full herein.

90. The Computer Fraud & Abuse Act (as amended by Identity Theft Enforcement & Restitution Act of 2008, P.L. No. 110-326) ("CFAA") authorizes federal criminal penalties against a person who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer. 18 U.S.C. § 1030(a)(2)(C) (2009).

91. CFAA also authorizes federal criminal penalties against a person who knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer. 18 U.S.C. § 1030(a)(5)(A) (2009).

92. CFAA also authorizes federal criminal penalties against a person who intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damages and loss. 18 U.S.C. § 1030(a)(5)(C) (2009).

93. Plaintiff's cellular telephone and the wireless devices of the members of the Class are "protected computers" within the meaning of CFAA because they (a) are used exclusively by or for a financial institution or the United States Government; (b) are used by or for a financial institution or the United States Government and Defendants' conduct affected that particular use; and/or (c) are used in or affecting interstate or foreign commerce or communication. 18 U.S.C. §§ 1030(e)(2)(A)-(B) (2009).

94. Defendants knowingly and/or intentionally accessed without authorization and/or exceeded authorized access to Plaintiff's cellular telephone and the wireless devices of the members of the Class by sending them unauthorized Watch List Alert text messages, thereby obtaining information from those wireless devices.

95. WSOD acted without authorization in accessing Plaintiff's cellular telephone and the wireless devices of the members of the Class by sending them unauthorized text messages because Plaintiff and the members of the Class never granted WSOD permission to access their wireless devices by sending unauthorized text messages to their wireless devices. In addition, the lack of prior authorization by Plaintiff and the members of the Class is supported by the myriad attempts Plaintiff made *after* receiving the unauthorized text messages from WSOD to stop receiving future unauthorized text messages from WSOD,

96. WSOD obtained information from Plaintiff's cellular telephone and the wireless devices of the members of the Class in the form of information that the wireless devices were active and functioning, and the general or actual geographic location of Plaintiff's cellular telephone and the wireless devices of the members of the Class. Upon information and belief, WSOD used or could have used the information obtained from Plaintiff's cellular telephone and the wireless devices of the members of the Class to sell, license, or otherwise market the wireless numbers of Plaintiff and the members of the Class to its clients or affiliates interested in sending related text-message content to Plaintiff and the members of the Class.

97. WSOD also obtained information from Plaintiff's cellular telephone and the wireless devices of the members of the Class in the form of temporarily or permanently obtaining a portion of the finite storage capacity of Plaintiff's cellular telephone and the wireless devices of the members of the Class.

98. Defendants also knowingly caused the transmission of a code or information in the form of Watch List Alert SMS text-message content to Plaintiff's cellular telephone and the wireless devices of the members of the Class and, as a result, intentionally caused damage without authorization to Plaintiff's cellular telephone and the wireless devices of the members of the Class, as "damage" is defined specifically in CFAA.

99. Defendants also intentionally accessed without authorization Plaintiff's cellular telephone and the wireless devices of the members of the Class by sending them unauthorized Watch List Alert text messages, and, as a result of such conduct, caused

damages and loss to Plaintiff and the members of the Class, as those terms are defined specifically in CFAA.

100. For example, the unauthorized text messages Plaintiff and the members of the Class received from WSOD caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by depleting or "using up" the wireless devices' finite RAM or ROM causing the electronic operations and functioning of the wireless devices to slow or lag in operation, which impaired the integrity and availability of data, program(s), system(s), or information found in or on Plaintiff's cellular telephone and the wireless devices of the members of the Class.

101. The unauthorized text messages Plaintiff received from WSOD also caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by misallocating, interfering, or depleting the limited wireless bandwidth of the wireless devices that would have otherwise been dedicated to other wireless operations such as the telephone calls, internet access, instant messaging, or the sending or receiving of legitimate text messages by Plaintiff and the members of the Class, which impaired the integrity and availability of data, program(s), system(s), or information found in or on Plaintiff's cellular telephone and the wireless devices of the members of the Class.

102. The unauthorized text messages Plaintiff received from WSOD also caused damage to Plaintiff's cellular telephone and the wireless devices of the members of the Class by temporarily and/or permanently misallocating, depleting, or consuming the finite permanent or "hard drive" memory storage capacity of Plaintiff's cellular telephone and the wireless devices of the members of the Class, which caused Plaintiff's cellular

telephone and the wireless devices of the members of the Class to slow or lag in operation and functioning, which impaired the integrity and availability of data, program(s), system(s), or information found in or on Plaintiff's cellular telephone and the wireless devices of the members of the Class.

103. Plaintiff and the members of the Class also suffered a "loss" (as defined by CFAA) as the result of receiving unauthorized text messages from WSOD because Plaintiff and the members of the Class were forced, among other things, to take various remedial actions and measures at a cost to Plaintiff and the members of the Class, including, in Plaintiff's case, hiring an attorney to stop WSOD from sending future unauthorized text messages, to remedy the interruption of service to Plaintiff's cellular telephone and the wireless devices of the members of the Class caused by WSOD's unauthorized text messages, as described more fully above.

104. CFAA provides: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g) (2009).

105. As a result of Defendants' violation of CFAA, Plaintiff and the members of the Class have suffered, and will continue to suffer, among other things, economic damages, the aggregate amount of which is at least $5,000, as provided for in 18 U.S.C. §1030(c)(4)(A)(i)(I) (2009).

COUNT II
COMMON LAW TRESPASS TO CHATTELS
(AGAINST ALL DEFENDANTS)

106. Plaintiff restates and realleges paragraphs 1-105 above as though set forth in full herein.

107. Plaintiff's cellular telephone and the wireless devices of the members of the Class are protected property interests.

108. Defendants and/or their agents, knowingly, intentionally, and/or negligently, and without authorization or consent from Plaintiff and the members of the Class, gained access to Plaintiff's cellular telephone and the wireless devices of the members of the Class, used Plaintiff's cellular telephone and the wireless devices of the other members of the Class, occupied the memory of those wireless devices, dispossessed and interfered with the unencumbered access of Plaintiff and the members of Class to their wireless devices, and actually impaired Plaintiff's cellular telephone and the wireless devices of the members of the Class.

109. For example, by sending unauthorized text messages to Plaintiff's cellular telephone and the wireless devices of the members of the Class, WSOD knowingly, intentionally, and/or negligently dispossessed and interfered with the unencumbered access of Plaintiff and the members of the Class to their wireless devices, and/or actually impaired Plaintiff's cellular telephone and the wireless devices of the members of the Class because the text messages (1) depleted or "used up" the finite RAM or ROM of the wireless devices causing the electronic operations and functioning of the wireless devices to slow or lag in operation; (2) misallocated, interfered with, or depleted the limited

wireless bandwidth of the wireless devices that otherwise would have been dedicated to other wireless operations of Plaintiff and the members of the Class such as telephone calls, internet access, instant messaging, and/or the sending or receiving of legitimate text messages; and (3) temporarily and/or permanently misallocated, depleted, or consumed the finite permanent or "hard drive" storage capacity of Plaintiff's cellular telephone and the wireless devices of the members of the Class, which caused Plaintiff's cellular telephone and the wireless devices of the members of the Class to slow or lag in operation or functioning.

110. In doing so, Defendants knowingly, intentionally, and/or negligently interfered with, dispossessed or intermeddled with, and/or deprived Plaintiff and the members of the Class of the use of their wireless devices, or a part thereof, and/or actually impaired Plaintiff's cellular telephone and the wireless devices of the members of the Class.

111. Defendants were not justified in knowingly, intentionally, and/or negligently interfering with, dispossessing or intermeddling with, and/or depriving Plaintiff and the members of the Class of the use of their wireless devices, or a part thereof, and/or were not justified in actually impairing Plaintiff's cellular telephone and the wireless devices of the members of the Class.

112. As a result of Defendants' interference with, dispossession, intermeddling, or deprivation of the use of the wireless devices of Plaintiff and the members of the Class, and/or the actual impairment of Plaintiff's cellular telephone and the wireless

devices of the members of the Class, Plaintiff and the members of the Class have suffered, and will continue to suffer, damages.

COUNT III
COMMON LAW UNJUST ENRICHMENT
(AGAINST ALL DEFENDANTS)

113. Plaintiff restates and realleges paragraphs 1-112 above as though set forth in full herein.

114. Plaintiff and the members of the Class have conferred a direct benefit on Defendants. Defendants have received and retained money, through a profit share or otherwise, belonging to Plaintiff and the Class resulting from Defendants' conduct of causing them to be billed for unauthorized text-messaging charges, and, in particular, their practice of systematically, repeatedly, and without authorization, causing Plaintiff and the Class of wireless-device users to be billed by their wireless carriers for mobile-content services and text messages authorized by the previous subscriber of recycled telephone numbers.

115. For example, Defendants have been unjustly enriched at Plaintiff's and the Class's expense as the result of the text message fees generated by WSOD by sending unauthorized text messages to Plaintiff and the members of the Class, and the unlawfully retained profit made by WSOD from its text-messaging-content contracts with its clients and affiliates, which contracts were premised on sending as many text messages as possible to wireless-device users despite the fact that WSOD knew that many of these users never authorized WSOD to send them text messages.

116. WSOD also has been unjustly enriched at Plaintiff's expense in particular because each text message WSOD sent to Plaintiff's cellular telephone depleted the total number of text messages she was able to send or receive during any particular month, regardless of whether she exceeded her limit of text messages per month. The value to Plaintiff of a particular text message is quantifiable because she paid a flat monthly fee for 300 text messages per month.

117. Defendants appreciate or have knowledge of this benefit and the fact that some of the monies they have received and continue to receive are the result of unauthorized text-messaging charges generally, and recycled wireless-telephone numbers in particular.

118. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and the members of the Class, which Defendants have been unjustly enriched as a result of Defendants' actions more fully described above.

119. As a result of Defendants' retention of money belonging to Plaintiff and the other members of the Class, Plaintiff and the members of the Class have suffered, and will continue to suffer, damages.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff Brenda Czech, on behalf of herself and the Class, requests the following relief:

1. An order certifying the Class as defined above;

2. An award of actual, compensatory, and/or statutory damages;

3. An injunction requiring Defendants to cease transmitting Watch List Alert text-message content to those wireless-device users who have not authorized or consented to receiving such text messages;

4. Reasonable attorney's fees and costs; and

5. Such further and other relief the Court deems appropriate, including imposition of a constructive trust.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Respectfully submitted,

Dated: August 10, 2009

LOCKRIDGE GRINDAL NAUEN P.L.L.P.

/s/ Matthew R. Salzwedel

Robert K. Shelquist (MN #021310X)
Matthew R. Salzwedel (MN #0312903)
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 339-0981
rkshelquist@locklaw.com
mrsalzwedel@locklaw.com

Myles McGuire
Steven Lezell
KamberEdelson, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370
Fax: (312) 589-6378
mmcguire@kamberedelson.com
slezell@kamberedelson.com

Attorneys for Brenda Czech, individually, and on behalf of a class of similarly situated individuals